CA2182598

Publication Title:

CELLULAR RADIOTELEPHONE SYSTEM WITH REMOTELY PROGRAMMED MOBILE STATIONS

Abstract:

Abstract of CA2182598

A cellular radiotelephone system (10) includes mobile stations (28) which may be remotely programmed from a customer activation system (12) to effect activation and other programming needs. Mobile stations (28) are manufactured in a blank form that causes them to operate only in an inactive state. During activation, information describing the mobile station's electronic serial number (ESN) is collected along with area of use information. A mobile identification number (MIN) is assigned in response to the area of use information. A page message is directed to the mobile station operating in its inactive state, but the page message references the mobile station's ESN. While inactive, the mobile station (28) detects pages directed to its ESN. A remote programming session is then performed wherein digital user-specific programming data, including the newly assigned MIN, are transferred to the mobile station (28) over a voice channel using a control channel protocole (80).

(19) Canadian Intellectual Property Office / Office de la Propriété Intellectuelle du Canada
An Agency of Industry Canada / Un organisme d'Industrie Canada

(11) CA 2 182 598 (13) C

(40) 26.08.2003
(43) 31.08.1995
(45) 26.08.2003

(12)

(21) 2 182 598

(22) 31.01.1995

(51) Int. Cl.[6]: H04Q 7/22

(85) 01.08.1996

(86) PCT/US95/01266

(87) WO95/023487

(30) 08/201,445 US 24.02.1994
08/315,010 US 29.09.1994

(72) ZICKER, ROBERT G. (US).
DION, JOHN K. (US).

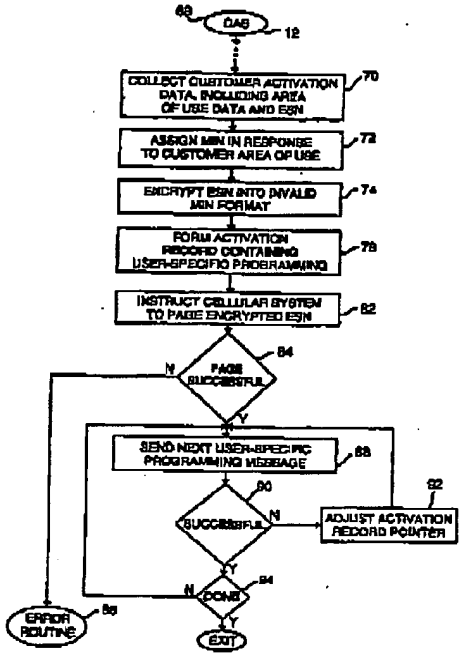
(73) GTE WIRELESS SERVICE CORPORATION
245 Perimeter Center Parkway ATLANTA XX (US).

(74) BORDEN LADNER GERVAIS LLP

(54) SYSTEME RADIOTELEPHONIQUE CELLULAIRE A POSTES MOBILES PROGRAMMES A DISTANCE
(54) CELLULAR RADIOTELEPHONE SYSTEM WITH REMOTELY PROGRAMMED MOBILE STATIONS

(57)

This invention provides a cellular radiotelephone system which includes mobile stations which may be remotely programmed from a customer activation system to effect activation and other programming needs. Mobile stations are manufactured in a blank form that causes them to operate only in an inactive state. During activation, information describing the mobile station's electronic serial number (ESN) is collected along with area of use information. A mobile identification number (MIN) is assigned in response to the area of use information. A page message is directed to the mobile station operating in its inactive state, but the page message references the ESN of the mobile station. While inactive, the mobile station detects pages directed to its ESN. A remote programming session is then performed wherein digital user-specific programming data, including the newly assigned MIN, are transferred to the mobile station over a voice channel using a control channel protocol. A novel cellular telephone which is configured for such remote activation, as well as the methods of remote activation are also provided.



Un organisme d'Industrie Canada / An agency of Industry Canada

(12) BREVET CANADIEN
CANADIAN PATENT
(13) C

(86) Date de dépôt PCT/PCT Filing Date: 1995/01/31
(87) Date publication PCT/PCT Publication Date: 1995/08/31
(45) Date de délivrance/Issue Date: 2003/08/26
(85) Entrée phase nationale/National Entry: 1996/08/01
(86) N° demande PCT/PCT Application No.: US 1995/001266
(87) N° publication PCT/PCT Publication No.: 1995/023487
(30) Priorités/Priorities: 1994/02/24 (08/201,445) US; 1994/09/29 (08/315,010) US

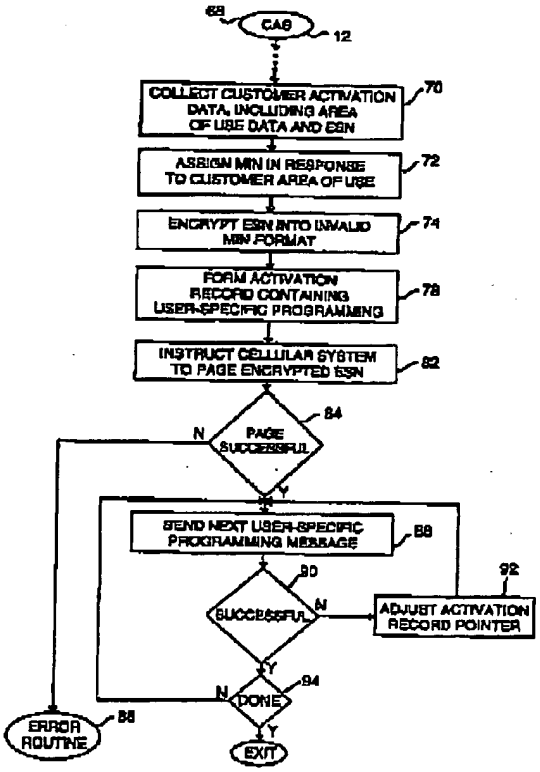
(51) Cl.Int.^{6}/Int.Cl.^{6} H04Q 7/22

(72) Inventeurs/Inventors:
ZICKER, ROBERT G., US;
DION, JOHN K., US

(73) Propriétaire/Owner:
GTE WIRELESS SERVICE CORPORATION, US

(74) Agent: BORDEN LADNER GERVAIS LLP

(54) Titre : SYSTEME RADIOTELEPHONIQUE CELLULAIRE A POSTES MOBILES PROGRAMMES A DISTANCE
(54) Title: CELLULAR RADIOTELEPHONE SYSTEM WITH REMOTELY PROGRAMMED MOBILE STATIONS



(57) Abrégé/Abstract:
This invention provides a cellular radiotelephone system which includes mobile stations which may be remotely programmed from a customer activation system to effect activation and other programming needs. Mobile stations are manufactured in a

(13) C

(57) Abrégé(suite)/Abstract(continued):
blank form that causes them to operate only in an inactive state. During activation, information describing the mobile station's electronic serial number (ESN) is collected along with area of use information. A mobile identification number (MIN) is assigned in response to the area of use information. A page message is directed to the mobile station operating in its inactive state, but the page message references the ESN of the mobile station. While inactive, the mobile station detects pages directed to its ESN. A remote programming session is then performed wherein digital user-specific programming data, including the newly assigned MIN, are transferred to the mobile station over a voice channel using a control channel protocol. A novel cellular telephone which is configured for such remote activation, as well as the methods of remote activation are also provided.

ABSTRACT

This invention provides a cellular radiotelephone system which includes mobile stations which may be remotely programmed from a customer activation system to effect activation and other programming needs. Mobile stations are manufactured in a blank form that causes them to operate only in an inactive state. During activation, information describing the mobile station's electronic serial number (ESN) is collected along with area of use information. A mobile identification number (MIN) is assigned in response to the area of use information. A page message is directed to the mobile station operating in its inactive state, but the page message references the ESN of the mobile station. While inactive, the mobile station detects pages directed to its ESN. A remote programming session is then performed wherein digital user-specific programming data, including the newly assigned MIN, are transferred to the mobile station over a voice channel using a control channel protocol. A novel cellular telephone which is configured for such remote activation, as well as the methods of remote activation are also provided.

(a) TITLE OF THE INVENTION

CELLULAR RADIOTELEPHONE SYSTEM WITH REMOTELY PROGRAMMED MOBILE STATIONS

(b) TECHNICAL FIELD TO WHICH THE INVENTION RELATES

The present invention relates generally to cellular radio telecommunication systems. More specifically, the present invention relates to the control of user-specific programming which is stored in, and which is acted upon, by mobile stations.

(c) BACKGROUND ART

Mobile stations which are used in connection with conventional cellular telecommunication systems are manufactured in a blank or unprogrammed state. An activation procedure is performed both to acquire customer identification information so that customers may be successfully billed for communication services, and to personalize the mobile stations so that they will be capable of providing communication services. Until a mobile station has been activated, it can neither make nor receive a call. After activation, changes in either customer preferences or system operating characteristics can require changes to the personalization of the mobile stations.

Personalization is accomplished by causing the mobile station to include certain user-specific programming. The user-specific programming represents data which cause the mobile station to function as desired for a specific user. Examples of user-specific programming include, but are not limited to, a mobile identification number (MIN) and home system identification (SID). The MIN represents the phone number of the mobile station, and the home SID represents the identification of the cellular system with which the user has contracted to provide communication services.

Activation is currently accomplished through two different techniques. In accordance with one activation technique, a skilled service representative collects data from a new customer, uses a computer in data communication with an on-line computerized customer activation system to obtain a valid MIN, and manually operates the keypad of the mobile station to program the MIN and other user-specific programming in the mobile station. In accordance with the second technique, preprogrammed mobile stations are stocked in retail

stores so that no user specific programming need be keyed into the mobile station keypad. Both techniques have undesirable consequences.

The technique of requiring a skilled service representative to program mobile stations forces new customers to go out of their way to visit a service representative. This is an inconvenience to customers and limits the availability of mobile stations in mass markets. Moreover, this technique is error prone because the human factor is involved in hand-keying user-specific programming into mobile stations. It is also expensive because of labor costs which are associated with making a sufficient number of skilled service representatives available to the general public. In addition, the expense and error-prone nature of this technique are exacerbated because the programming sequences are typically cryptic, different mobile station manufactures use different programming sequences, and the programming sequences change as new mobile station models become available.

The second technique of stocking preprogrammed mobile stations addresses some of the problems associated with using skilled service representatives to hand-key user-specific programming into mobile stations. However, this second technique increases activation costs due to the need to inventory and track mobile stations that differ only in their user-specific programming. In addition, user-specific programming is typically configured to fit general customer profiles rather than the preferences of individual customers. It also leads to confusion in the assignment of MINs. For example, MINs are assigned well in advance of when the mobile station is actually sold. The MIN is allocated for a particular area or location of use, typically at the location of the retain store where the mobile station is sold. However, the customer may seldom or never actually use the mobile station near that retail store. Consequently, the customer may get a mobile station with a MIN which is not appropriate for the actual area of use of the customer.

The problems associated with the above two techniques for activating mobile stations could, in large part, be eliminated through the use of a remotely programmable mobile station. While a few remotely programmable mobile stations have been devised, they cannot be remotely programmed for activation. Conventional remotely programmable mobile stations require the mobile station to be activated before they may be remotely programmed. Prior activation is required because the mobile stations accomplish remote programming by making or receiving a call, but they can neither make nor receive a call until after activation. In addition, conventional remotely programmable mobile stations use ubiquitous telecommunications modem technology to receive the user-specific data. A security risk results due to the coupling of mobile stations to a public network and the widespread availability of modem technology in the general population.

(d) DESCRIPTION OF THE INVENTION

Accordingly, it is an object of a first aspect of the present invention to provide an improved cellular system having remotely programmed mobile stations.

An object of a second aspect of the present invention is remotely to programme mobile stations for user-specific activation programming and for subsequent alterations in the user-specific programming.

An object of a third aspect of the present invention is to provide remote programming without requiring the use of ubiquitous conventional telecommunications modem technology.

An object of a fourth aspect of the present invention is to provide for the secure remote programming of certain mobile stations without requiring significant changes to the existing cellular telecommunications infrastructure.

A first broad aspect of this invention provides an improvement in a cellular radio telecommunications system which activates mobile stations from locations remote to the mobile stations. The improvement consists of a mobile station comprising a memory having a first storage location containing data describing a location-independent identifying code for the mobile station, and additional storage locations. The mobile station includes a receiver which is configured to receive digital data. The mobile station includes a transmitter which is configured to transmit digital data. Finally, the mobile station includes a controller which is coupled to the memory, to the receiver, and to the transmitter. The controller is configured to evaluate a page message which references the location-independent identifying code and to engage in a remote programming session in which user-specific programming is received at the mobile station and is stored in the additional storage locations.

By a first variant of this first broad aspect of this invention, the memory is configured so that the first storage location resides in a read only component of the memory, and the additional storage locations reside in a read/write component of the memory.

By a second variant of this first broad aspect of this invention, and/or a variant of this first variant thereof, the location-independent identifying code represents an electronic serial number (ESN) that uniquely identifies the mobile station, and the controller is

configured to decrypt the signalling data to determine whether the page message references the ESN. By a first variation thereof, the user-specific programming includes a mobile identification number (MIN), the MIN being a telephone number for the mobile station, and the controller is configured to evaluate signalling data to detect a message which references the MIN after performing the remote programming session.

A second broad aspect of this invention provides a method of operating a cellular telecommunications system to manage mobile identification number (MIN) programming which is stored in mobile stations, to manage signalling between at least one land station and the mobile stations, and to manage the transfer of user information to, and from, the mobile stations. The method includes the steps of establishing a communication between a land station and a mobile station using a mode selected from a digital data mode and an analog audio mode. The method further includes operating the land station in cooperation with the mobile station so that the selected digital data mode is used to communicate both signalling and the MIN programming. The method finally includes operating the land station in cooperation with the mobile station so that the selected analog audio mode is used to communicate the user information.

By a first variant of this second broad method aspect of this invention, the method includes providing the MIN or a telephone number which is assigned to the mobile station, storing an electronic serial number (ESN) in the mobile station and in order uniquely to identify the mobile station, operating the mobile station in an inactive state wherein the mobile station does not have a valid MIN but has an ESN, operating the mobile station in an active state wherein the mobile station has a valid MIN, and signalling pages which are directed to the mobile station using data which is selected from data which reference the MIN and data which reference the ESN. By a first variation thereof, the method additionally comprises the steps of encrypting the ESN to obtain the signalling data which reference the ESN, and decrypting the signalling data which reference the ESN to determine whether the signalling data are directed to the mobile station.

By a second variant of this second broad method aspect of this invention, and/or a variants of this first variant thereof, the method includes selecting the MIN to be a telephone number which is assigned to the mobile station, storing an electronic serial number (ESN) in the mobile station in order uniquely to identify the mobile station,

operating the mobile station in an inactive state wherein the mobile station does not have a valid MIN but has an ESN in an active state wherein the mobile station has a valid MIN, operating the land station only in the digital data mode to communicate with the mobile station when the mobile station is operating in the inactive state, and operating the land station in both the digital data mode and the analog audio mode to communicate with the mobile station when the mobile station is operating in the active state.

By a third variant of this second broad method aspect of this invention, and/or variants of the above variants thereof, the method includes selecting the MIN to be a telephone number which is assigned to the mobile station, operating the mobile station in an inactive state wherein the mobile station does not have a valid MIN, operating the mobile station in an active state wherein the mobile station has a valid MIN, and sending, to the mobile station, MIN programming which causes the mobile station to invalidate the MIN and thereafter to operate in the inactive state.

By a fourth variant of this second broad method aspect of this invention, and/or variants of the above variants thereof, the method includes operating the system to communicate a first portion of the signalling in the digital data mode using a control channel protocol over control channels, operating the system to communicate a second portion of the signalling in the digital data mode using a voice channel protocol over voice channels, operating the system to communicate the user information in the analog audio mode over the voice channels, and transferring the MIN programming to the mobile station using the control channel protocol over one of the voice channels. By a first variation thereof, the method additionally comprises the steps of paging the mobile station over one of the control channels using the control channel protocol, instructing the mobile station to tune to the one voice channel, transmitting a digital synchronizing signal over the one voice channel, tuning the mobile station to the one voice channel, synchronizing the mobile station to the synchronizing signal, and transmitting the MIN programming to the mobile station over the one voice channel using the control channel protocol.

A third broad aspect of this invention provides a method of operating a cellular telecommunications system to manage user-specific programming which is stored in a mobile station having an electronic serial number (ESN) stored therein which uniquely identifies the mobile station, the user-specific programming including a mobile

identification number (MIN), the MIN being a telephone number which is assigned to the mobile station so that the mobile station operates in an inactive state wherein the mobile station does not have a valid MIN but has an ESN and in an active state wherein the mobile station has a valid MIN, the method comprising the steps of establishing a communication between the land station and the mobile station using a mode selected from a digital data mode and an analog audio mode, operating the land station in cooperation with the mobile station so that the selected digital data mode is used to communicate both signalling and the user-specific programming, operating the land station in cooperation with the mobile station so that the selected analog audio mode is used to communicate the user information, using the MIN to signal calls directed to the mobile station when the mobile station operates in the active state, and using the ESN to signal calls directed to the mobile station when the mobile station operates in the inactive state.

A fourth broad aspect of this invention provides a method of activating a cellular mobile station from a location remote to the mobile station, the method comprising the steps of storing, in the mobile station, data describing a location-independent identifying code for the mobile station, receiving page signalling messages at the mobile station, evaluating the page signalling messages to detect a page which references the location-independent identifying code, and engaging, in response to the page, in a remote programming session in which user-specific programming is received at and stored in the mobile station.

By a first variant of this fourth broad method aspect of this invention, the method includes providing the location-independent identifying code as an electronic serial number (ESN). By a first variation thereof, the method includes operating the engaging step to assign a mobile identification number (MIN) to the mobile station, the MIN being a telephone number for the mobile station, operating the mobile station in an inactive state prior to activation, operating the mobile station in an active state after activation, and paging the mobile station using data which reference the MIN when the mobile station is operating in the active state.

By a second variant of this fourth broad method aspect of this invention, and/or a variant of this first variant thereof, the method additionally comprises the step of

encrypting the ESN, and transmitting a page signalling message which conveys the ESN in an encrypted form.

By a third variant of this fourth broad method aspect of this invention, and/or variants of the above variants thereof, the method includes engaging the mobile station in signalling communications, user-specific programming communications, and user information communications, operating in a digital data mode to communicate both the signalling communications and the user-specific programming communications, and operating in an analog audio mode to communicate the user information. By a first variation thereof, the method includes operating the mobile station to cooperate with a cellular system to exchange a first portion of the signalling communications over control channels in the digital data mode using a control channel protocol, to exchange a second portion of the signalling communications over a voice channel in the digital data mode using a voice channel protocol, and to exchange the user information over the voice channels in the analog audio mode, and transferring the user-specific programming to the mobile station using the control channel protocol over one of the voice channels.

By a fourth variant of this fourth broad method aspect of this invention, and/or variants of the above variants thereof, the method additionally comprising the steps of paging the mobile station over one of the control channels using the control channel protocol, instructing the mobile station to tune to the one voice channel, transmitting a digital synchronizing signal over the one voice channel, tuning the mobile station to the one voice channel, synchronizing the mobile station to the synchronizing signal, and transmitting the user-specific programming to the mobile station over the one voice channel using the control channel protocol.

A fifth broad aspect of this invention provides a cellular telephone which is configured for remote activation, the cellular telephone comprising an antenna, a transmitter which is coupled to the antenna, a receiver which is coupled to the antenna, a controller which is coupled to the transmitter and to the receiver, and a memory which is coupled to the controller, wherein the controller is configured to detect a page message which is received over a cellular network, the page message referencing a location-independent identifying code stored in the memory.

A sixth broad aspect of this invention provides a cellular telephone which is configured for remote activation, the cellular telephone comprising an antenna;

a transmitter which is coupled to the antenna, a receiver which is coupled to the antenna, the receiver being configured to conduct telephone calls, a controller which is coupled to the transmitter and to the receiver, and a memory which is coupled to the controller; wherein the controller is configured to detect a page message received at the receiver and referencing a location-independent identifying code stored in the memory.

By a first variant of these fifth and sixth broad aspects of this invention, the location-independent identifying code is derived from an electronic serial number (ESN) assigned to the cellular telephone.

By a second variant of these fifth and sixth broad aspects of this invention, and/or a variant of this first variant thereof, the controller is further configured to enter a remote programming mode after detecting the page message.

By a first variation thereof, after entering the remote programming mode, the controller is configured to accept digital data received by the cellular telephone and to store the digital data in the memory. By a second variation thereof, the digital data comprises a home system identification number (SID) for the cellular telephone. By a third variation thereof, the digital data comprises a system identification number (SID). By a fourth variation thereof, the digital data comprises a mobile identification number (MIN) for the cellular telephone. By a fifth variation thereof, the digital data comprises an executable instruction.

A seventh broad aspect of this invention provides a cellular telephone comprising an antenna, a transmitter which is coupled to the antenna, a receiver which is coupled to the antenna, so that the antenna, the transmitter, and the receiver form an air interface for the cellular telephone, a controller which is coupled to the air interface, and a memory which is coupled to the controller, wherein the controller is configured to detect a page message received from a cellular network by the air interface, the page message referencing a location-independent identifying code stored in the memory.

An eighth broad aspect of this invention provides a cellular telephone comprising an antenna, a transmitter which is configured to conduct telephone calls, the transmitter being coupled to the antenna, a receiver which is configured to conduct telephone calls, the

receiver being coupled to the antenna and to the antenna, the transmitter and the receiver forming an air interface for the cellular telephone, a controller which is coupled to the air interface, and a memory which is coupled to the controller, wherein the controller is configured to detect a page message received through the receiver by the air interface, the page message referencing a location-independent identifying code stored in the memory.

By a first variant of these seventh and eighth broad aspects of this invention, the location-independent identifying code is derived from an electronic serial number (ESN) of the cellular telephone. By a first variation thereof, after detecting the page message, the controller is further configured to receive remote programming information received by the air interface. By a second variation thereof, the remote programming information comprises a mobile identification number (MIN). By a third variation thereof the controller is configured to store the received mobile identification number (MIN) in the memory.

A ninth broad aspect of this invention provides a cellular telephone which is configured for network initiated activation, the cellular telephone comprising an antenna, a transmitter which is coupled to the antenna, a receiver which is coupled to the antenna a controller which is coupled to the transmitter and to the receiver, and a memory which is coupled to the controller, the memory containing an electronic serial number (ESN) which is assigned to the cellular telephone but not containing a mobile identification number (MIN) which is assigned to the cellular telephone, wherein the controller is configured to detect a page message that references data derived from the electronic serial number (ESN) and to enter a remote programming mode after detecting the page message.

By a first variant of this ninth broad aspect of this invention, the controller is configured to accept digital data which is received by the cellular telephone while the controller is in the remote programming mode.

A tenth broad aspect of this invention provides a cellular telephone which is configured for network initiated activation, the cellular telephone comprising an antenna, a transmitter which is coupled to the antenna, a receiver which is coupled to the antenna, a memory containing a location-independent identifying code, and first means for detecting a page message which references the location-independent identifying code.

By a first variant of this tenth broad aspect of this invention, and/or variants of the above variants thereof, the cellular telephone further includes second means for entering a remote programming mode after the first means has detected the page message. By a first variation thereof, the cellular telephone is configured to receive digital data while in the remote programming mode and to store the digital data in the memory.

By a second variant of this tenth broad aspect of this invention, and/or a variant of this first variant thereof, the digital data comprises a mobile identification number (MIN).

By a third variant of this tenth broad aspect of this invention, and/or variants of the above variants thereof, the digital data comprises a system identification number (SID).

By a fourth variant of this tenth broad aspect of this invention, and/or variants of the above variants thereof, the digital data comprises an executable instruction.

An eleventh broad aspect of the present invention provides a cellular telephone which is configured for remote reprogramming, the cellular telephone comprising an antenna, a receiver which is coupled to the antenna, a transmitter which is coupled to the antenna, a controller which is coupled to the transmitter and to the receiver, and a memory which is coupled to the controller, the memory containing an electronic serial number (ESN) and a first valid mobile identification number (MIN) for the cellular telephone; and the controller is configured to accept digital data which is received over a cellular network by the receiver operating in a digital data mode and to store the digital data in the memory.

A twelfth broad aspect of the present invention provides a cellular telephone which is configured for network initiated remote programming, the cellular telephone comprising, an antenna, a transmitter which is coupled to the antenna, a receiver which is coupled to the antenna, the receiver being configured to conduct telephone calls, a controller which is coupled to the transmitter and to the receiver, and a memory which is coupled to the controller, and the controller is configured to detect a digital message which is received by the receiver and to enter a remote programming mode after detecting the digital message.

A thirteenth broad aspect of the present invention provides a cellular telephone which is configured for network initiated remote programming, the cellular telephone comprising, an antenna, a transmitter which is coupled to the antenna, a receiver which is coupled to the antenna, a memory containing an electronic serial number (ESN) and a first mobile identification number (MIN), first means for detecting a digital message received by the

receiver, and second means for entering a remote programming mode wherein the cellular telephone receives digital data which is formatted according to a control channel protocol, the second means entering the remote programming mode after the first means detects the digital message.

By a first variant of these twelfth and thirteenth broad aspects of this invention, and/or variants of the above variants thereof, the receiver is configured to receive the digital data formatted according to a control channel protocol. By a first variation thereof, the digital data comprises a second mobile identification number (MIN), the second MIN being different than the first MIN. By a second variation thereof, the digital data comprises a second mobile identification number (MIN). By a third variation thereof, the controller is further configured to accept digital programming data received by the receiver while in the remote programming mode and to store the digital programming data in the memory.

By a second variant of these twelfth and thirteenth broad aspects of this invention, and/or variants of the above variants thereof, the digital data comprises a system identification number (SID).

By a third variant of these twelfth and thirteenth broad aspects of this invention, and/or variants of the above variants thereof, the digital programming data comprises a mobile identification number (MIN).

By a fourth variant of these twelfth and thirteenth broad aspects of this invention, and/or variants of the above variants thereof, the digital programming data comprises an executable instruction.

By a fifth variant of these twelfth and thirteenth broad aspects of this invention, and/or variants of the above variants thereof, the digital data comprises data that deactivates the cellular telephone.

By a sixth variant of these twelfth and thirteenth broad aspects of this invention, and/or variants of the above variants thereof, the digital data comprises a deactivation command.

By a seventh variant of these twelfth and thirteenth broad aspects of this invention, and/or variants of the above variants thereof, the digital data is conveyed to the cellular telephone through a remote programming session initiated by the cellular network.

By a eighth variant of these twelfth and thirteenth broad aspects of this invention, and/or variants of the above variants thereof, the digital message is initiated by the network.

A fourteenth broad aspect of this invention provides a cellular telephone which is configured for remote activation, the cellular telephone comprising, an antenna, a transmitter which is coupled to the antenna, a receiver which is coupled to the antenna, a controller which is coupled to the transmitter and to the receiver, and a memory which is coupled to the controller, the controller is configured to detect a page message that references a location-independent identifying code stored in the memory, and the location-independent identifying code is derived from an electronic serial number (ESN) which is assigned to the cellular telephone.

By a first variant of this fourteenth broad aspect of this invention, the controller is further configured to enter a remote programming mode after detecting the page message.

By a first variation thereof, after entering the remote programming mode, the controller is configured to accept digital data which is received by the cellular telephone and to store the digital data in the memory. By a second variation thereof, the digital data comprises a home system identification number (SID) for the cellular telephone. By a third variation thereof, the digital data comprises a system identification number (SID). By a fourth variation thereof, the digital data comprises a mobile identification number (MIN) for the cellular telephone. By a fifth variation thereof, the digital data comprises an executable instruction.

A fifteenth broad aspect of this invention provides a cellular telephone comprising an antenna, a transmitter which is coupled to the antenna, a receiver which is coupled to the antenna so that the antenna, the transmitter, and the receiver form an air interface for the cellular telephone, a controller which is coupled to the air interface, and a memory which is coupled to the controller, the controller is configured to detect a page message which is received by the air interface, the page message referencing a location-independent identifying code which is stored in the memory, and the location-independent identifying code is derived from an electronic serial number (ESN) of the cellular telephone.

By a first variant of this fifteenth broad aspect of this invention, after detecting the page message, the controller is further configured to receive remote programming information received by the air interface.

By a first variation thereof, the remote programming information comprises a mobile identification number (MIN). By a second variation thereof, the controller is configured to store the received mobile identification number (MIN) in the memory.

A sixteenth broad aspect of this invention provides a remotely programmable cellular radiotelephone device comprising, a first memory location for storing a unique telephone serial number, a second memory location which is programmed with an initial identification number wherein the initial identification number is associated with the telephone serial number, transceiver means for transmitting and receiving cellular radiotelephone communication signals to and from a cellular system, and programming means for reprogramming the second memory location in response to receipt of a mobile identification number from the transceiver means so that the second memory location is programmed with the mobile identification number.

An eighteenth broad aspect of this invention provides a remotely programmable cellular radiotelephone device comprising, a non-programmable memory for storing a unique telephone serial number, a programmable memory which is programmed with an initial identification number, and the initial identification number comprises digits from the telephone serial number, transceiver means for transmitting and receiving cellular radiotelephone communication signals to and from a cellular system, and programming means for reprogramming the programmable memory in response to receipt of a mobile identification number from the transceiver means so that the programmable memory location is programmed with the mobile identification number.

By a first variant of these seventeenth and eighteenth broad aspects of the unique telephone serial number is an electronic serial number (ESN) of the cellular radiotelephone service.

By a second variant of these seventeenth and eighteenth broad aspects of this invention, and/or a variant of this first variant thereof, the transceiver means comprises page receiving means for receiving a data communication message from the cellular

system, and the radiotelephone device is identified by the initial identification number and the data communication message comprises the mobile identification number.

A nineteenth broad aspect of this invention provides a wireless telephone which is configured for activation through an activation call originated from a location remote to the wireless telephone, the wireless telephone comprising, an antenna, a transmitter which is coupled to the antenna, the transmitter being configured to conduct user information calls, a receiver which is coupled to the antenna, the receiver being configured to conduct the activation call and the user information calls, a controller, which is coupled to the transmitter and to the receiver, and a memory which is coupled to the controller, and the controller is configured to detect a page message received at the receiver during origination of the activation call and referencing a location-independent identifying code stored in the memory.

A twentieth broad aspect of this invention provides a method for remotely programming a cellular radiotelephone device which includes a programmable memory, the cellular radiotelephone device being programmed with a unique initial identification number, the remotely programming method comprising the steps of, providing the unique initial identification number to a cellular system, establishing a data communication session from the cellular system to the cellular radiotelephone device using the unique initial identification number to identify the cellular radiotelephone device, transmitting data to the cellular radiotelephone device during the session, wherein the data comprises a mobile identification number; and reprogramming the cellular radiotelephone device so that the cellular radiotelephone device is programmed with the mobile identification number.

By a first variant of this twentieth broad method aspect of this invention, the method includes providing the cellular radiotelephone device with a first memory location for storing a unique telephone serial number, and associates the initial identification number with the telephone number.

A twenty-first broad aspect of this invention provides a method for remotely programming a cellular radiotelephone device which includes a programmable memory which is programmed with a unique initial identification number, the remotely programming method comprising the steps of, providing the unique initial identification number to a cellular system, establishing a data communication session from the cellular

system to the cellular radiotelephone device using the unique initial identification number to identify the cellular radiotelephone, transmitting data to the cellular radiotelephone device during the session, wherein the data comprises a mobile identification number, and reprogramming the programmable memory so that the programmable memory is programmed with the mobile identification number.

By a first variant of this twenty-first broad method aspect of this invention, the method includes the step of providing the radiotelephone device with a non-programmable memory for storing a unique telephone serial number, wherein the initial identification number comprises digits from the telephone number.

By a second variant of these twentieth and twenty-first broad method aspects of this invention, and/or a variant of this first variant thereof, the method includes providing the telephone serial number in the form of an electronic serial number of the radiotelephone device.

By a third variant of these twentieth and twenty-first broad method aspects of this invention, and/or variants of the above variants thereof, the providing step further comprises the step of providing the telephone serial number to the cellular system, and the providing step is followed by the step of comparing the telephone serial number and the initial identification number.

By a fourth variant of these twentieth and twenty-first broad method aspects of this invention, and/or variants of the above variants thereof, the providing step further comprises providing data other than the unique initial identification number to the cellular system. By a first variation thereof, the providing step is followed by the step of controlling the activation of the radiotelephone device.

(e) DESCRIPTION OF THE FIGURES

In the accompanying drawings,

FIG. 1 shows a telecommunications system which may incorporate one embodiment of an aspect of the present invention;

FIG. 2 shows a block diagram of a mobile station configured in accordance with an embodiment of an aspect of the present invention;

FIG. 3 shows a flow chart of a process performed by a customer activation system (CAS);

FIG. 4 shows a data format diagram of a three word page response message sent over a reverse control channel;

FIG. 5 shows a data stream protocol diagram of a control channel protocol;

FIG. 6 shows a flow chart of a method performed by a land station;

FIG. 7 shows a data format diagram of a two word mobile station control message sent over a forward control channel;

FIG. 8 shows a flow chart of a method performed by a mobile station;

FIG. 9 shows a data stream protocol diagram of a voice channel protocol; and

FIG. 10 shows a flow chart of a method performed by the mobile station during a remote programming session.

(f) AT LEAST ONE MODE FOR CARRYING OUT THE INVENTION

FIG. 1 shows a block diagram of a telecommunications system 10 which may incorporate an embodiment of one aspect of the present invention. Telecommunications system 10 includes a customer activation system (CAS) 12 with any number of service representative operator stations 14 located nearby. CAS 12 is implemented using a conventional computer system. Operator stations 14 couple to a public switched telecommunications network (PSTN) 16 or other communications network through a conventional local loop so that a service representative

may engage in telephonic voice conversations with customers and prospective customers. CAS 12 couples to a trunk 20 supplied through PSTN 16. Any number of additional telecommunications devices 22 may also couple to PSTN 16 to engage in the communication of audio, video, data, or other user information.

PSTN 16 desirably extends trunk 20 to a mobile telecommunications switching office (MTSO) 24. For the most part, MTSO 24 has a conventional structure and performs methods which are conventional in the art of cellular telephony, and more particularly in accordance with conventional cellular telephony standards established for the United States of America and other countries, as set forth in Standard EIA-553 and elsewhere. MTSO 24 couples to any number of land stations 26, which likewise have generally conventional structures and generally perform conventional methods. However methods performed by MTSO 24 and land stations 26 diverge from conventional methods in the manner set forth below. Land stations 26 may represent cell sites, base stations, and the like, which may manage radio communications over control channels and/or voice channels so that mobile stations 28 may receive telecommunications services. However, land stations 26 are not limited to use only as a cell site but may also be used for a personal or private communications system. In addition, while the "land station" terminology is consistent with the conventional cellular telephony lexicon, land stations are not limited to being coupled to land lines and may couple to MTSO 24 or other controlling stations through RF links.

Mobile stations 28 may communicate user information through the voice channels to other mobile stations 28, telecommunications devices 22, or even operator station 14. Generally, mobile stations 28 are intended to be used while in motion or during halts at unspecified points. However, mobile stations 28 include hand-held units, vehicle-mounted units, portable units, and units which are physically configured for use only at permanent stationary locations.

User information is communicated when a call is setup and a land station 26 and mobile station 28 operate in an analog audio mode to communicate analog audio signals. Consequently, voice communications are directly translated into electronic user information, and digital data may be translated into electronic user information through the use of modems (not shown) which translate digital data into analog audio signals.

Likewise, mobile stations 28 may transmit and receive digital signalling data. Signalling data are generally communicated to allocate and otherwise manage the channels over which communications are to take place and to indicate a desire to engage in transmitting user information over the voice channels. Generally, signalling data are transparent to users. Signalling data are communicated when a land station 26 and mobile station 28 operate in a digital data mode to communicate digital data. In the preferred embodiment, digital signalling data are communicated using a 10 Kbit, Manchester encoded, FSK digital communication scheme which is well known in the cellular telephony art.

In accordance with broad aspects of the present invention, user-specific programming is communicated between CAS 12 and mobile stations 28. User-specific programming generally represents digital data and/or executable instructions which personalize or otherwise configure a mobile station 28 so that it may be used to communicate user information and otherwise provide communication services in a manner desired by a customer. Examples of typical user-specific programming include a mobile identification number (MIN), home system identification (SID), "A" or "B" system selection criteria, feature package identification, local area dialing rules, and the like. In addition, user-specific programming may include programming instructions which are executed by a microprocessor within mobile station 28 to cause mobile station 28 to function in any particular manner. Further, for purposes of aspects of the present invention, user-specific programming also includes an instruction which, when executed by a mobile station 28, deactivates the mobile station 28 so that it cannot be used to communicate user information. User-specific programming is communicated when a land station 26 and mobile station 28 operate in a digital data mode to communicate digital data using the 10 Kbit communication scheme that conventional cellular telephony devices are designed to accommodate. Thus, no extra modems are required to communicate user-specific programming, the expense of the extra modems may be eliminated, and the security risk of being vulnerable to unwanted programming through ubiquitous modem technology available throughout the world is avoided.

Mobile stations 28 may be remotely programmed even to effect their own activation. Desirably, mobile stations 28 are manufactured, distributed, stocked, and sold in a blank, unpersonalized form where they are configured to operate only in an inactive mode. Mobile stations 28 may include certain default user-specific programming which may make mobile station 28 usable, although not necessarily as desired by certain customers.

However, inactive mobile stations 28 do not include a valid MIN. Those skilled in the art will appreciate that a MIN represents a telephone number assigned to a mobile station 28. The MIN is desirably assigned based upon the area of use of the customer for the mobile station 28. For example, area codes and central office codes need to correspond to the locations where the mobile station 28 is most likely to be used so that the mobile station 28 will not be roaming and otherwise get assessed with excessive fees for the majority of calls and so that incoming calls may be successfully routed to the mobile station 28. Thus, a valid MIN is assigned in the course of activating a mobile station 28, and this MIN is a location-dependent code consistent with an area code and central office code corresponding to the areas where mobile station 28 will most likely be used. PSTN 16 uses the MIN in routing calls to particular MTSOs 24, and cellular systems use MINs to route calls to and from specific mobile stations 28.

While an inactive mobile station 28 does not have a MIN or at least a valid MIN, it does have an electronic serial number (ESN). The ESN uniquely identifies the mobile station 28 to any cellular system and is configured so that it may not be readily changed. The ESN is assigned in accordance with a code of the manufacturer and another code which is unique to the

manufacturer. The ESN does not designate any area of use and is therefore a location-independent code which conveys no information useful to PSTN 16 in routing calls to the mobile station 28 to which it is assigned.

FIG. 1 shows a sales kiosk 30 which may be used in the activation of a mobile station 28'. Sales kiosk 30 and CAS 12 are typically remotely located from one another, and may in some situations be located thousands of miles away from one another. Desirably, sales kiosk 30 may be located in a retail store where mobile stations 28 are sold to mass markets, and any number of sales kiosks 30 may be supported by CAS 12.

Sales kiosk 30 represents a telecommunications device which couples to PSTN 16 through a local loop. When a customer wishes to purchase mobile station 28', the customer may physically take mobile station 28' to sales kiosk 30 and use sales kiosk 30 to engage in a voice conversation through PSTN 16 with a service representative at a station 14. Through this voice conversation, the service representative may collect user activation information from the customer and enter this information into CAS 12. Such information includes the identifying data which permits a cellular service provider to successfully bill for communication services. It also includes the ESN for mobile station 28', which a customer may, for example, recite from reading a tag affixed to mobile station 28'. In addition, the activation information includes location data which inform the service representative where mobile station 28' is most likely to be used. This information may be inferred from the address of the customer and the address of sales kiosk 30, and/or directly obtained from a conversation with the customer. Through the voice conversation, the customer may select preferred feature packages and the like.

When the activation information has been gathered, and preferably while the voice conversation is ongoing, CAS 12 automatically causes an "activation call" to be placed to mobile station 28'. The appropriate MTSO 24 to use for this call is selected by CAS 12 in response to an address of the sales kiosk 30 where mobile station 28' is currently located. Methods which are discussed below are performed in CAS 12, MTSO 24, land stations 26, and mobile station 28' so that mobile station 28' will recognize and respond to the call by using a paging message which references the mobile station's ESN. Once a data link is established, a remote programming session is performed where user-specific programming, including a newly assigned MIN, is transferred to mobile station 28' and stored therein. At the conclusion of the remote programming session, mobile station 28' may be used to communicate user information.

FIG. 2 shows a block diagram of electronic hardware included in a mobile station 28 which is configured in accordance with the requirements of system 10. An antenna 32 of mobile station 28 couples to a first port of a duplexer 34, while a second port of duplexer 34 is adapted to receive a modulated RF signal provided by a transmitter 36 and a third port of duplexer 34 provides a received RF signal to an input of a receiver 38. An audio output from receiver 38 couples to a speaker 40, and an audio input to transmitter 36 couples to a microphone 42. Transmitter 36 receives analog audio signals from microphone 42 and

receiver 38 provides analog audio signals to speaker 40 when mobile station 28 operates in its analog audio mode. Although not shown, a modem may couple to or otherwise be switched into these analog audio paths so that digital data converted into an analog audio form may be communicated in a conventional manner while mobile station 28 operates in its analog audio mode.

A controller 44 controls the operation of mobile station 28. Controller 44 may be implemented using one or more commercially available microprocessors. Controller 44 provides controlling signals to transmitter 36 and to receiver 38 over data lines 46 and 48, respectively. In addition, controller 44 provides digital data to a digital data input 50 of transmitter 36 for transmission while mobile station 28 operates in its digital data mode and receives digital data from a digital data output 52 of receiver 38 while mobile station 28 operates in its digital data mode. In the preferred embodiment, the controlling signals applied over data lines 46 and 48 identify frequency channels to which transmitter 36 and receiver 38 are instructed to tune, and they specify whether transmitter and receiver 36 and 38, respectively, are to operate in the analog audio mode or digital data mode.

A display 54 couples to controller 44 and visually shows information provided thereto by controller 44. A keypad 56 couples to controller 44 so that controller 44 may detect key presses and then appropriately respond to the key presses. A timer 58 couples to controller 44 and helps controller 44 monitor the passage of time. In addition, a memory 60 couples to controller 44. Memory 60 stores data, variables, tables, lists, and databases that are used in connection with the operation of mobile station 28. In addition, memory 60 stores programming instructions which are executed by controller 44 and define the various methods procedures, routines, tasks, and the like performed by controller 44 and mobile station 28. In the preferred embodiments, memory 60 is partitioned into three components. A random access memory (RAM) component 62 represents volatile read/write memory. An electrically erasable programmable read only memory (EEPROM) component 64 provides non-volatile read/write memory, and a read only memory (ROM) component 66 represents non-volatile, read only memory which cannot be easily erased or otherwise altered. Those skilled in the art will appreciate that ROM component 66 may be implemented using PROMS, EPROMS, and the like.

Desirably, default user-specific programming is stored both in ROM 66 and EEPROM 64 when mobile station 28 is manufactured and sold to a customer. This default user-specific programming includes an invalid MIN and an invalid home SID, along with a factory setting for a keypad lock code and an index to a predetermined default features package. Due at least in part to the use of an invalid MIN, mobile station 28 cannot engage in calls which communicate user information at this point. ROM 66 also stores the location-independent ESN for mobile station 28 and data identifying all control channels used by "A" and "B" cellular systems.

FIG. 3 shows a flow chart of a method 68 performed by customer activation system (CAS) 12. CAS method is performed when user-specific programming needs to be remotely programmed into one or more mobile stations 28, such as may occur during activation. While FIG. 3 specifically illustrates program flow for an activation, a similar method may be followed for other remote programming sessions which may occur after activation. As indicated by ellipsis in FIG. 3, method 68 may perform many tasks which are not directly related to writing user-specific programming to mobile stations 28. Such tasks may include the capture and maintenance of customer identification and billing records.

Method 68 performs a task 70 to collect customer activation data. This activation data desirably include information describing the area where the mobile station 28 will most often be used, where the mobile station 28 is currently located, the ESN of the mobile station, and other data. Task 70 may be performed with the cooperation of a service representative who is engaging in a voice telephone conversation with a customer who may be located at a sales kiosk 30 (see FIG. 1).

After task 70, a task 72 assigns a valid MIN to the mobile station 28 in response to the area of use identified above in task 70. This area of use may, but need not, include the location of sales kiosk 30. The assigned MIN represents a 10 digit phone number that is not currently in use elsewhere, and has an area code and office code consistent with the MTSO 24 (see FIG. 1) for this area of use. Next, a task 74 encrypts the ESN of the mobile station into an invalid MIN format.

FIG. 4 shows a data format diagram of a three word page response message 76 sent by a mobile station 28 over a reverse control channel to a land station 26. Message 76 follows conventional cellular telephony standards. As FIG. 4 illustrates, the MIN is formatted as a 34-bit binary number having a first portion (MIN1) conveyed by a first word and a second portion (MIN2) conveyed by a second word. The ESN is a 32-bit binary number that is conveyed in a third word.

Referring back to FIG. 3, task 74 applies the 32-bit ESN of the mobile station to an encryption algorithm which generates a 34-bit encrypted ESN-MIN, and the 34-bit ESN-MIN is formatted as though it were an invalid MIN. The use of an invalid MIN format guarantees that no activated mobile station 28 will accidentally recognize the encrypted ESN as its MIN. An invalid MIN may be obtained by, for example, forcing the first digit of the decimal form of the ESN-MIN to a value of zero. The particular encryption algorithm implemented at task 74 is not relevant to various aspects of the present invention, and this algorithm may use conventional public or private key encrypting techniques. As discussed below in more detail, the ESN-MIN will be used in lieu of a MIN to page the mobile station 28. The use of encryption further enhances security by reducing the risk of third party meddling with mobile station programming.

After task 74, a task 78 forms an activation record containing all the user-specific programming to be written into the mobile station 28 in an upcoming remote programming session. Desirably, the activation record is made up of one or more words, where each word

includes a parameter identity (PID) and parameter value (PVAL). The MIN assigned above in task 72 to mobile station 28 represents one of the parameters conveyed in a word, and the activation record may include any number of words. Various PID/PVAL words may also be coded to present instructions to mobile station 28 rather than raw parameter data. Such instructions may, for example, instruct mobile station 28 that the previous PID/PVAL word was the last word to be transferred in the remote programming session. In another example, a PID/PVAL word may be coded as a command to deactivate mobile station 28 and thereby undo the user-specific programming specified in a previous activation.

In addition, task 78 arranges the PID/PVAL words in accordance with a mobile station control message delivered using a control channel protocol 80. FIG. 5 shows a data stream protocol diagram of control channel protocol 80 for a message that conveys one word of data. Protocol 80 is a conventional user-inaccessible protocol used in cellular telephony for control channel digital data communication. It conveys one 40-bit word for each 463-bit message. As illustrated in FIG. 5, protocol 80 includes a 10-bit dotting sequence plus a busy/idle bit, followed by an 11-bit word sync pattern plus a busy/idle bit, followed by five interleaved repetitions of an "A" stream 40-bit word and a "B" stream 40-bit word, wherein a busy/idle bit is inserted for each 10 bits of the A and B stream words. Conventionally, the "A" stream is distinguished from the "B" stream by the least significant bit (LSB) of the MIN to which the streams are directed. Thus, task 78 may repeat the PID/PVAL words in the "A" or "B" stream per protocol 80 and the LSB of the ESN-MIN generated in task 74 (see FIG. 3), or task 78 may simply repeat each PID/PVAL word ten times in each message. Control channel protocol 80 is executed on an assigned voice channel so that user-specific programming may be quickly transferred using as few system resources as possible. The entire method of remotely activating a mobile station 28 should take only a few seconds once the customer activation information has been collected.

After task 78, a task 82 selects an appropriate MTSO 24 (see FIG. 1) based upon the current location of the mobile station 28 to be remotely programmed, establishes a data link to this MTSO 24, and instructs the MTSO and cellular system it controls to page the ESN-MIN number generated above in task 74. From the perspective of the cellular system, the ESN-MIN is treated as a valid MIN, and a conventional paging process is performed. CAS method 68 performs a task 84 to determine whether the page is eventually successful. If not successful, program control passes to an error handling routine 86 so that an appropriate action may be taken. For the above described activation method a customer is engaged in an ongoing conversation with a service representative, and the error routine 86 may simply inform the service representative of the problem. For other remote programming situations, the unsuccessful page may simply be logged for queuing again at a later time.

When the page is successful, a task 88 sends the next user-specific programming message from the activation record formed above in task 78 through trunk 20, PSTN 16, MTSO 24, and a land station 26 (see FIG. 1) to mobile station 28. After task 88, a query task

90 waits for either an acknowledgment (ACK) or no acknowledgment (NAK) response from mobile station 28. Based on the nature of the received response, if any, task 90 determines whether the prior message was successful. If it was not successful, a task 92 adjusts a pointer to the activation record formed in task 78 to repeat the last record, and program control loops back to task 88. Although not shown, this loop may include additional tasks to break the loop should an excessive number of unsuccessful attempts be made.

When task 90 determines that the last message was successfully delivered, a query task 94 determines whether the final message from the activation record has been delivered. So long as additional messages remain, program control loops back to task 88 to continue sending PID/PVAL word messages to mobile station 28. When finished, program control exits method 68 and mobile station 28 has been remotely activated.

Method 68 also may be used to remotely program mobile stations 28 which are currently activated. For post-activation remote programming, task 70 may gather the user-specific programming to be downloaded into the mobile station 28. Tasks 72 and 74 may substitute the existing MIN of the mobile station for the encrypted ESN-MIN discussed above After task 74 program flow prpceeds as described above, and the mobile station 28 will be paged using its MIN. Method 68 may also be repetitively performed remotely to program entire populations of mobile stations 28. This situation may occur when a cellular system change takes place, e.g., assigning new area codes or central office codes to a cellular system. In this situation, an entire population of mobile stations 28 requires updated user-specific programming reflecting newly assigned MINs. Method 68 may be repeated for each mobile station 28. Task 70 obtains a new MIN, tasks 72 and 74 identify an old MIN, and program flow proceeds as described above, but is repeated for each mobile station 28 in the population.

FIG. 6 shows a flow chart of a method 96 performed by a land station 26. While method 96 is directed toward a single land station 26, those skilled in the art will appreciate that portions of it may be performed by the MTSO 24 which controls it and by other land stations 26 which are also controlled by that MTSO 24. As indicated by ellipsis in FIG. 6, method 96 includes many tasks related to managing channels that are allocated to land station 26 and are conventional in cellular telephony. A query task 98 is performed to signal when the land station 26 receives a page instruction from CAS 12 (see FIGs. 1 and 3). So long as no such instruction is received, land station 26 continues to perform conventional cellular land station processes.

Desirably, when the page instruction is received, all land stations in the cellular system controlled by MTSO 24 simultaneously receive the same instruction. At this point, a task 100 pages the "MIN" specified in the instruction with a local control order "tune and sync" message. As discussed above, it may be either a valid MIN or the ESN-MIN number discussed above in connection with task 74 (see FIG. 3). Land station 26 uses a conventional mobile station control message, e.g., message 102 shown in FIG. 7, and delivers message

102 while operating in its digital mode over a control channel using control channel protocol 80 (see FIG. 5).

Referring briefly to FIGs. 6 and 7, task 100 configures mobile station control message 102 as a local control order page message by inserting the MIN, which may be the ESN-MIN during an activation, in MIN1 and MIN2 fields of first and second words, by setting an appropriate value (11110) in the order field, and by setting the local field to a code that mobile station 28 will interpret as a tune and sync command.

Referring back to FIG. 6, after task 100 pages the MIN or ESN-MIN obtained from CAS 12, a query task 104 determines whether a page response message 76 (see FIG. 4) was received from the mobile station 28. As shown in FIG. 4, the page response message includes the MIN or ESN-MIN so that land station 26 can verify that it responded to the previous local control order page message. If no page response message is received, program control loops back to task 100. Although not shown, additional tasks may be included to break this loop after a certain number of repeated paging attempts have been tried or if an instruction to do so is received via MTSO 24.

When task 104 detects a page response message 76 (see FIG. 4) that responds to the tune and sync local control order page message transmitted above at task 100, a task 106 finds an idle voice channel, marks the channel busy so that it will not get assigned to other mobile stations 28, and transmits a digital synchronizing signal over the selected voice channel. Moreover, task 106 transmits the synchronizing signal on the voice channel using control channel protocol 80 (see FIG. 5). Task 106 may, for example, continuously transmit its overhead message over this voice channel. While task 106 causes land station 26 to operate one of its voice channels somewhat like a control channel, nothing requires any alteration in the manner in which land station 26 operates its control channel. In other words, control channel overhead and control channel messages continue to be transmitted from land station 26 over its control channel.

After task 106, a task 108 transmits a voice channel assignment message over its control channel using the conventional channel assignment protocol. Next, a query task 110 causes land station 26 to monitor the voice channel assigned above in task 106 for a ready message transmitted by mobile station 28. The ready message is sent to land station 26 using a reverse control channel protocol even though this is a voice channel. Program control stays at task 110 until this ready message is received. However, error handling tasks (not shown) may be included to address the situation where the mobile station 28 fails to respond with the ready message.

When task 110 detects the ready message, a task 112 is performed to patch the voice channel to trunk 20 (see FIG. 1) and to inform CAS 12 (see FIG. 1) that the page was successful. At this point, CAS 12 controls the data link to mobile station 28. Land station 26 exerts no further influence over the remote programming session. Rather, CAS 12 controls the remote programming session as discussed above in connection with FIG. 3. Land station 26

merely performs a query task 114 to determine when trunk 20 goes inactive. When trunk 20 is dropped, land station 26 performs a task 116 to tear down the call to mobile station 28. As a result of tearing down the call, the voice channel becomes idle again and may be used as needed to convey user information to and from mobile stations 28.

FIG. 8 shows a flow chart of a method 118 performed by a mobile station 28. Method 118 may be performed when mobile station 28 powers up. Mobile station 28 performs various initialization tasks, including a task 120 which causes it to operate in its digital data mode. As discussed above in connection with FIG. 2, in this mode digital data, rather than analog audio signals, are routed through transmitter 36 and receiver 38. After task 120, a query task 122 determines whether mobile station 28 is active. Task 122 may, for example, determine whether its user-specific programming includes a valid MIN, but other evaluations can lead to the same conclusion. If mobile station 28 has not been activated, then it will operate in its inactive state, and program control proceeds to a task 124.

Task 124 scans control channels, the identities of which are programmed into mobile station 28, to select a best server control channel. Task 124 may monitor a received signal strength indicator (RSSI) when tuned to a control channel to determine whether any received signal exhibits sufficient strength.

After task 124, a task 126 performs a decryption operation which complements the encryption operation discussed above in connection with task 74 (see FIG. 3). The decryption operation may be performed in at least two different ways. The ESN of the mobile station may be encrypted in a manner similar to that discussed above in connection with task 74 so that a resulting encrypted ESN-MIN is generated by task 126. This ESN-MIN may be compared with MINs conveyed from land stations 26 in page messages. Alternately, MINs may be parsed from received page messages and subjected to algorithms which complement the encryption algorithm performed by CAS 12 in task 74. This "decrypted" MIN may then be compared to the mobile station's ESN.

After task 126, a query task 128 determines whether a tune and sync-local control order page message received from the control channel references the ESN of the mobile station Mobile station 28 may continue to monitor paging messages received over the selected control channel for a few seconds before task 128 decides that no page directed to its ESN has been received. When task 128 makes this determination, program control loops back to task 124 to select a different control channel and repeat the process of monitoring for a page message directed to the mobile station's ESN. In the preferred embodiment, the control channels selected at task 124 alternate between A and B cellular systems, and task 124 may select not only the control channels in each system with the strongest signals, but the control channels with the next strongest signals.

As discussed above, page messages directed to the mobile station may be simultaneously transmitted from all land stations 26 within a particular cellular system. Thus, a good chance exists that a page will be detected within a few tries. When task 128 detects an

ESN referenced tune and sync local control order page message, a task 130 returns the appropriate page response message 76 (see FIG. 4) over the reverse control channel. The page response message echoes the ESN-MIN for the mobile station's MIN in the response message, and may include the mobile station's ESN.

After task 130, a query task 132 causes mobile station 28 to wait until the voice channel assignment message is received over the control channel. However, additional tasks may cause program control to exit task 132 if a voice channel assignment message is not forthcoming. In addition, additional tasks may evaluate received messages to determine if some other message or command directed to mobile station 28 is received. When the voice channel assignment message is detected, a task 134 is performed to tune transmitter 36 and receiver 38 (see FIG. 2) to the specified voice channel. After task 134, a query task 136 monitors the digital data signals and messages received over the voice channel until synchronization has been achieved. When mobile station 28 is synchronized to the digital data being transmitted over the voice channel, a task 138 returns the ready message to the land station 26 over the voice channel using a reverse control channel protocol which is normally used only on control channels.

After task 138, program control proceeds to a remote programming session 140, which is discussed in more detail below. During remote programming session 140 mobile station 28 continues to operate in its digital mode and its inactive state. Through remote programming session 140, user-specific programming will be communicated to mobile station 28 over the voice channel using control channel protocol 80 (see FIG. 5). Upon successful completion of a remote programming session 140, mobile station 28 may be activated and will thereafter operate in its active state. In its active state, mobile station 28 may operate in either its analog audio mode or its digital data mode.

Referring back to task 122, when mobile station 28 decides that it is active, it operates in its active state to perform numerous tasks, as indicated by ellipsis, which are conventional for cellular mobile stations. These tasks include monitoring control channels to detect incoming calls, tracking changes in channel availability, and monitoring keypad 56 (see FIG. 2) for user input. A query task 142 represents one such conventional mobile station task. Task 142 determines whether a MIN referenced page has been received at mobile station 28. In other words, task 142 determines whether a page message received at mobile station 28 conveys the MIN assigned to mobile station 28 through activation.

When task 142 detects a MIN referenced page, a query task 143 determines whether the page is a tune and sync local control order page message. The local control order page message differs from a page order in that the page order informs mobile station 28 of an incoming call and the tune and sync local control order page message informs mobile station 28 of an upcoming remote programming session. If task 143 detects a tune and sync local control order page message, program control proceeds to task 130 to return the page response message and proceed with tuning and synchronizing to a voice channel as discussed above.

If task 143 determines that the page message was not a tune and sync local control order page message, then a query task 144 determines whether an incoming user information call is indicated through a page order message. If a user information call is not indicated, then program control proceeds to task 132 further to process the page message to determine what sort of communication has been received. If a user information call is indicated, then mobile station 28 returns a page response message (not shown) and otherwise handles the call in a conventional manner.

In particular, a task 146 causes mobile station 28 to operate in its analog audio mode, and a query task 148 causes mobile station 28 to remain in its analog audio mode until the call terminates. When the call terminates, mobile station 28 reverts back to its digital data mode of operation, as indicated in a task 150, and program control loops back to the task 142.

Mobile station 28 switches to its analog audio mode when it receives an instruction to switch to a voice channel. When operating in the analog audio mode, both digital data and analog audio communications may take place. The analog audio communications convey the user information and account for the vast majority of communications which may take place. However, a small amount of signalling may also take place using digital data communications. Such signalling includes the communication of hand off messages. Digital data communications which occur over the voice channel follow a voice channel protocol 152, as shown in FIG. 9. Voice channel protocol 152 differs significantly from control channel protocol 80 (see FIG. 5). Since a continuous stream of data are not provided over the voice channel, mobile station 28 does not have the opportunity to become well synchronized. Thus, voice channel protocol 152 includes a 101-bit dotting pattern followed by eleven repeats of a single 40-bit word interleaved with 37-bit dotting sequences and 11-bit word sync patterns. Voice channel protocol 152 conveys one 40-bit word using 1069 bits. Thus, digital data communication using voice channel protocol 152 has a greatly reduced data throughput compared to control channel protocol 80. On the other hand, only a very small amount of digital data are conveyed using protocol 152.

Accordingly, when mobile station 28 operates in its active state, it communicates using both the analog audio mode and the digital data mode. A very small amount of digital signalling data may be communicated in the analog audio mode, but data throughput suffers due the use of voice channel protocol 152 which accommodates an inability to achieve thorough synchronization. While FIG. 8 illustrates the detection of only MIN referenced pages when mobile station 28 operates in its active state, those skilled in the art will appreciate that nothing prevents additional tasks from being inserted which might also detect ESN referenced pages along the lines of tasks 126 and 128.

FIG. 10 shows a flow chart of remote programming session 140 performed by mobile station 28. Generally, remote programming session 140 responds to and complements the method performed by CAS 12 and discussed above in connection with FIG. 3. Substantially

the same method is performed whether mobile station 28 receives a MIN referenced page or an ESN referenced page.

Remote programming session 140 performs a task 153 to receive a message which conveys a PID/PVAL word from CAS 12. The PID/PVAL word is received over a voice channel using control channel protocol 80 (see FIG. 5). As discussed above, the PID/PVAL word is repeated several times in the received message, and task 153 may vote on the most likely data configuration, verify parity, and perform other verifications which evaluate whether the parameter value (PVAL) is compatible with the specified parameter ID (PID). The received PID/PVAL word is stored in a temporary buffer in memory 60 by a task 154, and a task 156 then returns either an acknowledgment (ACK) or no acknowledgment (NAK) message to tell CAS 12 whether to repeat the message or go on to the next message.

After task 156, a query task 158 determines whether the last received user-specific programming message conveyed an end session command. So long as this command has not been received, program control loops back to task 153. However, additional tasks (not shown) may be included to break the loop should no messages be received for an excessive duration.

When task 158 detects the end session command, a query task 160 determines whether the PID/PVAL words received include a deactivation command. If no deactivation command has been received, a task 162 saves the temporarily stored parameter values (PVALs) to the appropriate locations in non-volatile read/write component 64 of memory 60 (see FIG. 2). As discussed above, during activation remote programming sessions, a valid MIN and other parameters are down loaded to mobile station 28 through the remote programming session. Thus, task 162 causes the valid MIN and other parameters to be saved in memory 60. After task 162, program control exits remote programming session 140, and may proceed back to mobile station process 118 (see FIG. 8), where mobile station 28 will then operate in its active state.

When task 160 detects a deactivation command, a task 164 retrieves default user-specific programming from read only component 66 of memory 60. This default user-specific programming includes an invalid MIN, a default keypad lock code, and other default values. It has the effect of preventing mobile station 28 from communicating user information and forcing mobile station 28 to operate in its inactive state. After task 164, a task 166 saves this inactive user-specific programming in non-volatile read/write component 64 of memory 60, thereby overwriting any active user-specific programming which may have been previously stored there. After task 166, program control exits remote programming session 140 and may proceed back to mobile station process 118 (see FIG. 8), where mobile station 28 will then operate in its inactive state.

The inclusion of an inactive command, when coupled with the security precautions provided by aspects of the present invention, is advantageous for organizations which rent or loan mobile stations 28. The deactivation command helps such organizations maintain tight control over

their mobile stations 28 rendering the mobile stations 28 unusable when users are not complying with rental or loan arrangements.

While the remote programming session 140 discussed herein is configured to illustrate the writing of user-specific programming to mobile stations 28, nothing prevents remote programming session 140 from additionally being configured to read or audit data stored in mobile stations 28.

In summary, the present invention in its various aspects provides an improved cellular system having remotely programmable mobile stations. The mobile stations may be remotely programmed for user-specific activation programming and for subsequent alterations in the user-specific programming. The present invention in its various aspects provides remote programming without requiring the use of ubiquitous conventional telecommunications modem technology and without suffering the security risks associated therewith. In addition, the secure remote programming of certain mobile stations is achieved without significant changes to the existing cellular telecommunications infrastructure. Consequently, it may be successfully implemented at minimal expense.

The present invention has been described above with reference to preferred embodiments. However, those skilled in the art will recognize that changes and modifications may be made in these preferred embodiments without departing from the scope of various aspects of the present invention. For example, while aspects of the present invention have been described herein in connection with a particular cellular system, the present invention in other aspects may also be used in connection with a wide variety of cellular systems and other radio telecommunication systems. Furthermore, while aspects of the present invention has been descried in connection with a specific programming flow, those skilled in the art will appreciate that a large amount of variation in configuring process tasks and in sequencing process tasks may be directed to accomplishing substantially the same functions as are described herein.

CLAIMS

1. In a cellular radio telecommunications system which activates mobile stations from locations remote to said mobile stations, a mobile station comprising:

a memory having a first storage location containing data describing a location-independent identifying code for said mobile station, and additional storage locations;

a receiver which is configured to receive digital data;

a transmitter which is configured to transmit digital data; and

a controller which is coupled to said memory, to said receiver, and to said transmitter, said controller being configured to evaluate a page message which references said location-independent identifying code and to engage in a remote programming session in which user-specific programming is received at said mobile station and is stored in said additional storage locations.

2. The mobile station as claimed in claim 1, wherein said memory is configured so that said first storage location resides in a read only component of said memory and so that said additional storage locations reside in a read/write component of said memory.

3. A mobile station as claimed in claim 1 or claim 2 wherein:

said location-independent identifying code represents an electronic serial number (ESN) that uniquely identifies said mobile station; and

said controller is configured to decrypt said signalling data to determine whether said page message references said ESN.

4. A mobile station as claimed in claim 3, wherein:

said user-specific programming includes a mobile identification number (MIN), said MIN being a telephone number for said mobile station; and

said controller is configured to evaluate signalling data to detect a message which references said MIN after performing said remote programming session.

5. A method of operating a cellular telecommunications system to manage mobile identification number (MIN) programming stored in mobile stations, to manage signalling between one or more land stations and said mobile stations, and to manage the transfer of user information to and from said mobile stations, said method comprising the steps of:

communicating between a land station and a mobile station using a mode selected from a digital data mode and an analog audio mode;

operating said land station in cooperation with said mobile station so that said selected digital data mode is used to communicate both signalling and said MIN programming; and

operating said land station in cooperation with said mobile station so that said selected analog audio mode is used to communicate said user information.

6. A method as claimed in claim 5, including:

providing said MIN as a telephone number which is assigned to said mobile station;

storing an electronic serial number (ESN) in said mobile station in order uniquely to identify said mobile station;

operating said mobile station in an inactive state wherein said mobile station does not have a valid MIN but has an ESN, and operating said mobile station in an active state wherein said mobile station has a valid MIN; and

signalling pages which are directed to said mobile station using data which is selected from data which reference said MIN and data which reference said ESN.

7. A method as claimed in claim 6, additionally comprising the steps of:

encrypting said ESN to obtain said signalling data which reference said ESN; and

decrypting said signalling data which reference said ESN to determine whether said signalling data are directed to said mobile station.

8. A method as claimed in any one of claims 5 to 7, which includes:

providing said MIN as a telephone number which is assigned to said mobile station;

storing an electronic serial number (ESN) in said mobile station and in order uniquely to identify said mobile station;

operating said mobile station in an inactive state wherein said mobile station does not have a valid MIN but has an ESN, and operating said mobile station in an active state wherein said mobile station has a valid MIN;

operating said land station only in said digital data mode to communicate with said mobile station when said mobile station is operating in said inactive state; and

operating said land station in both said digital data mode and in said analog audio mode to communicate with said mobile station when said mobile station is operating in said active state.

9. A method as claimed in any one of claims 5 to 7 which includes:

providing said MIN as a telephone number which is assigned to said mobile station;

operating said mobile station in an inactive state wherein said mobile station does not have a valid MIN, and operating said mobile station in an active state wherein said mobile station has a valid MIN; and

sending, to said mobile station, MIN programming which causes said mobile station to invalidate said MIN and thereafter to operate in said inactive state.

10. A method as claimed in any one of claims 5 to 9, which include:

operating said system to communicate a first portion of said signalling in said digital data mode using a control channel protocol over control channels, to communicate a second portion of said signalling in said digital data mode using a voice channel protocol over voice channels, and to communicate said user information in said analog audio mode over said voice channels; and

transferring said MIN programming to said mobile station using said control channel protocol over one of said voice channels.

11. A method as claimed in claim 10, additionally comprising the steps of:

paging said mobile station over one of said control channels using said control channel protocol;

instructing said mobile station to tune to said one voice channel;

transmitting a digital synchronizing signal over said one voice channel;

tuning said mobile station to said one voice channel;

synchronizing said mobile station to said synchronizing signal; and

transmitting said MIN programming to said mobile station over said one voice channel using said control channel protocol.

12. A method of operating a cellular telecommunications system to manage user-specific programming which is stored in a mobile station having an electronic serial number (ESN) stored therein which uniquely identifies said mobile station, said user-specific programming including a mobile identification number (MIN), said MIN being a telephone number which is assigned to said mobile station so that said mobile station operates in an inactive state wherein said mobile station does not have a valid MIN but has an ESN and in an active state wherein said mobile station has a valid MIN, said method comprising the steps of:

communicating between said land station and said mobile station using a mode selected from a digital data mode and an analog audio mode;

operating said land station in cooperation with said mobile station so that said selected digital data mode is used to communicate both signalling and said user-specific programming;

operating said land station in cooperation with said mobile station so that said selected analog audio mode is used to communicate said user information;

using said MIN to signal calls directed to said mobile station when said mobile station operates in said active state; and

using said ESN to signal calls directed to said mobile station when said mobile station operates in said inactive state.

13. A method of activating a cellular mobile station from a location which is remote to said mobile station, said method comprising the steps of:

storing, in said mobile station, data describing a location-independent identifying code for said mobile station;

receiving page signalling messages at said mobile station;

evaluating said page signalling messages to detect a page which references said location-independent identifying code; and

engaging, in response to said page, in a remote programming session in which user-specific programming is received at and stored in said mobile station.

14. A method as claimed in claim 13, which comprising providing said location-independent identifying code as an electronic serial number (ESN).

15. A method as claimed in claim 14, including:

carrying out said engaging step to assign a mobile identification number (MIN) to said mobile station, said MIN being a telephone number for said mobile station;

operating said mobile station in an inactive state prior to activation and operating said mobile station in an active state after activation; and

paging said mobile station using data which reference said MIN when said mobile station is operating in said active state.

16. A method as claimed in claim 14 or claim 15, additionally comprising the step of:

encrypting said ESN; and

transmitting a page signalling message which conveys said ESN in an encrypted form.

17. A method as claimed in any one of claims 13 to 16, including

engaging said mobile station in signalling communications, user-specific programming communications, and user information communications,

operating said mobile station in a digital data mode to communicate both said signalling communications and said user-specific programming communications; and

operating said mobile station in an analog audio mode to communicate said user information.

18. A method as claimed in claim 17, including:

operating said mobile station to cooperate with a cellular system to exchange a first portion of said signalling communications over control channels in said digital data mode using a control channel protocol, to exchange a second portion of said signalling communications over a voice channel in said digital data mode using a voice channel protocol, and to exchange said user information over said voice channels in said analog audio mode; and

transferring said user-specific programming to said mobile station using said control channel protocol over one of said voice channels.

19. A method as claimed in any one of claims 13 to 18, additionally comprising the steps of:

paging said mobile station over one of said control channels using said control channel protocol;

instructing said mobile station to tune to said one voice channel;

transmitting a digital synchronizing signal over said one voice channel;

tuning said mobile station to said one voice channel;

synchronizing said mobile station to said synchronizing signal; and

transmitting said user-specific programming to said mobile station over said one voice channel using said control channel protocol.

20. A cellular telephone which is configured for remote activation, said cellular telephone comprising:

an antenna;

a transmitter which is coupled to said antenna;

a receiver which is coupled to said antenna;

a controller which is coupled to said transmitter and to said receiver; and

a memory which is coupled to said controller;

wherein said controller is configured to detect a page message which is received over a cellular network, said page message referencing a location-independent identifying code stored in said memory.

21. A cellular telephone which is configured for remote activation, said cellular telephone comprising:

an antenna;

a transmitter which is coupled to said antenna;

a receiver which is coupled to said antenna, said receiver being configured to conduct telephone calls;

a controller which is coupled to said transmitter and to said receiver; and

a memory which is coupled to said controller;

wherein said controller is configured to detect a page message received at said receiver and referencing a location-independent identifying code stored in said memory.

22. The cellular telephone of claim 20 or claim 21, wherein said location-independent identifying code is derived from an electronic serial number (ESN) assigned to said cellular telephone.

23. The cellular telephone of claim 20, claim 21 or claim 22, wherein said controller is further configured to enter a remote programming mode after detecting said page message.

24. The cellular telephone of claim 23, wherein, after entering said remote programming mode, said controller is configured to accept digital data received by said cellular telephone and to store said digital data in said memory.

25. The cellular telephone of claim 24, wherein said digital data comprises a home system identification number (SID) for said cellular telephone.

26. The cellular telephone of claim 24, wherein said digital data comprises a system identification number (SID).

27. The cellular telephone of claim 24, wherein said digital data comprises a mobile identification number (MIN) for said cellular telephone.

28. The cellular telephone of claim 24, wherein said digital data comprises an executable instruction.

29. A cellular telephone comprising:

an antenna;

a transmitter which is coupled to said antenna;

a receiver which is coupled to said antenna, so that said antenna, said transmitter, and said receiver form an air interface for said cellular telephone;

a controller which is coupled to said air interface; and

a memory which is coupled to said controller;

wherein said controller is configured to detect a page message which is received from a cellular network by said air interface, said page message referencing a location-independent identifying code stored in said memory.

30. A cellular telephone comprising:

an antenna;

a transmitter which is configured to conduct telephone calls, said transmitter being coupled to said antenna;

a receiver which is configured to conduct telephone calls, said receiver being coupled to said antenna and to said antenna, said transmitter and said receiver forming an air interface for said cellular telephone;

a controller which is coupled to said air interface; and

a memory which is coupled to said controller;

wherein said controller is configured to detect a page message received through said receiver by said air interface, said page message referencing a location-independent identifying code stored in said memory.

31. The cellular telephone of claim 29 or claim 30, wherein said location-independent identifying code is derived from an electronic serial number (ESN) of said cellular telephone.

32. The cellular telephone of claim 31, wherein after detecting said page message, said controller is further configured to receive remote programming information received by said air interface.

33. The cellular telephone of claim 32, wherein said remote programming information comprises a mobile identification number (MIN).

34. The cellular telephone of claim 33, wherein said controller is configured to store said received mobile identification number (MIN) in said memory.

35. A cellular telephone which is configured for network initiated activation, said cellular telephone comprising:

an antenna;

a transmitter which is coupled to said antenna;

a receiver which is coupled to said antenna;

a controller which is coupled to said transmitter and to said receiver; and

a memory which is coupled to said controller, said memory containing an electronic serial number (ESN) assigned to said cellular telephone but not containing a mobile identification number (MIN) assigned to said cellular telephone;

wherein said controller is configured to detect a page message that references data derived from said electronic serial number (ESN) and to enter a remote programming mode after detecting said page message.

36. The cellular telephone of claim 35, wherein said controller is configured to accept digital data which is received by said cellular telephone while said controller is in said remote programming mode.

37. A cellular telephone configured for network initiated activation, said cellular telephone comprising:

an antenna;

a transmitter which is coupled to said antenna;

a receiver which is coupled to said antenna;

a memory containing a location-independent identifying code; and

first means for detecting a page message which references said location-independent identifying code.

38. The cellular telephone of claim 37, further comprising:

second means for entering a remote programming mode after said first means has detected said page message.

39. The cellular telephone of claim 38, wherein said cellular telephone is configured to receive digital data while in said remote programming mode and to store said digital data in said memory.

40. The cellular telephone of any one of claims 35 to 39, wherein said digital data comprises a mobile identification number (MIN).

41. The cellular telephone of any one of claims 35 to 39, wherein said digital data comprises a system identification number (SID).

42. The cellular telephone of any one of claims 35 to 39, wherein said digital data comprises an executable instruction.

43. A cellular telephone which is configured for remote reprogramming, said cellular telephone comprising:

an antenna;

a receiver which is coupled to said antenna;

a transmitter which is coupled to said antenna;

a controller which is coupled to said transmitter and to said receiver; and

a memory which is coupled to said controller, said memory containing an electronic serial number (ESN) and a first valid mobile identification number (MIN) for said cellular telephone;

wherein said controller is configured to accept digital data which is received over a cellular network by said receiver operating in a digital data mode and to store said digital data in said memory.

44. A cellular telephone which is configured for network initiated remote programming, said cellular telephone comprising:

an antenna;

a transmitter which is coupled to said antenna;

a receiver which is coupled to said antenna, said receiver being configured to conduct telephone calls;

a controller which is coupled to said transmitter and to said receiver; and

a memory which is coupled to said controller;

wherein said controller is configured to detect a digital message which is received by said receiver and to enter a remote programming mode after detecting said digital message.

45. A cellular telephone which is configured for network initiated remote programming, said cellular telephone comprising:

an antenna;

a transmitter which is coupled to said antenna;

a receiver which is coupled to said antenna;

a memory containing an electronic serial number (ESN) and a first mobile identification number (MIN);

first means for detecting a digital message received by said receiver; and

second means for entering a remote programming mode wherein said cellular telephone receives digital data which is formatted according to a control channel protocol, said second means entering said remote programming mode after said first means detects said digital message.

46. The cellular telephone of claim 43 or claim 44, wherein said receiver is configured to receive said digital data which is formatted according to a control channel protocol.

47. The cellular telephone of claim 46, wherein said digital data comprises a second mobile identification number (MIN), said second MIN being different than said first MIN.

48. The cellular telephone of claim 46, wherein said digital data comprises a second mobile identification number (MIN).

49. The cellular telephone of claim 46, wherein said digital data comprises a system identification number (SID).

50. The cellular telephone of claim 46, wherein said digital programming data comprises a mobile identification number (MIN).

51. The cellular telephone of claim 46, wherein said digital programming data comprises an executable instruction.

52. The cellular telephone of claim 46, wherein said digital data comprises data that deactivates said cellular telephone.

53. The cellular telephone of claim 46, wherein said digital data comprises a deactivation command.

54. The cellular telephone of claim 46, wherein said digital data is conveyed to said cellular telephone through a remote programming session initiated by said cellular network.

55. The cellular telephone of any one of claims 45 to 54, wherein said controller is further configured to accept digital programming data which is received by said receiver while said receiver is in said remote programming mode and to store said digital programming data in said memory.

56. The cellular telephone of any one of claims 45 to 55, wherein said digital message is initiated by said network.

57. A cellular telephone which is configured for remote activation, the cellular telephone comprising:

an antenna;

a transmitter which is coupled to said antenna;

a receiver which is coupled to said antenna;

a controller which is coupled to said transmitter and to said receiver; and

a memory which is coupled to said controller; wherein said controller is configured to detect a page message that references a location-independent identifying code stored in said memory, and wherein said location-independent identifying code is derived from an electronic serial number (ESN) which is assigned to said cellular telephone.

58. The cellular telephone of claim 57, wherein said controller is further configured to enter a remote programming mode after detecting said page message.

59. The cellular telephone of claim 58, wherein, after entering said remote programming mode, said controller is configured to accept digital data which is received by said cellular telephone and to store said digital data in said memory.

60. The cellular telephone of claim 59, wherein said digital data comprises a home system identification number (SID) for said cellular telephone.

61. The cellular telephone of claim 59, wherein said digital data comprises a system identification number (SID).

62. The cellular telephone of claim 59, wherein said digital data comprises a mobile identification number (MIN) for said cellular telephone.

63. The cellular telephone of claim 59, wherein said digital data comprises an executable instruction.

64. A cellular telephone comprising:

an antenna;

a transmitter which is coupled to said antenna;

a receiver which is coupled to said antenna so that said antenna, said transmitter, and said receiver form an air interface for said cellular telephone;

a controller which is coupled to said air interface; and

a memory which is coupled to said controller;

wherein said controller is configured to detect a page message which is received by said air interface, said page message referencing a location-independent identifying code which is stored in said memory, and

wherein said location-independent identifying code is derived from an electronic serial number (ESN) of said cellular telephone.

65. The cellular telephone of claim 64, wherein after detecting said page message, said controller is further configured to receive remote programming information received by said air interface.

66. The cellular telephone of claim 64, wherein said remote programming information comprises a mobile identification number (MIN).

67. The cellular telephone of claim 65, wherein said controller is configured to store said received mobile identification number (MIN) in said memory.

68. A remotely programmable cellular radiotelephone device comprising:

a first memory location for storing a unique telephone serial number;

a second memory location which is programmed with an initial identification number wherein said initial identification number is associated with said telephone serial number;

transceiver means for transmitting and receiving cellular radiotelephone communication signals to and from a cellular system; and

programming means for reprogramming said second memory location in response to receipt of a mobile identification number from said transceiver means so that said second memory location is programmed with said mobile identification number.

69. A remotely programmable cellular radiotelephone device comprising:

a non-programmable memory for storing a unique telephone serial number;

a programmable memory which is programmed with an initial identification number, wherein said initial identification number comprises digits from said telephone serial number;

transceiver means for transmitting and receiving cellular radiotelephone communication signals to and from a cellular system; and

programming means for reprogramming said programmable memory in response to receipt of a mobile identification number from said transceiver means so that said programmable memory location is programmed with said mobile identification number.

70. A remotely programmable cellular radiotelephone device according to claim 68 or claim 69, wherein said unique telephone serial number is an electronic serial number (ESN) of said cellular radiotelephone service.

71. A remotely programmable cellular radiotelephone device according to claim 68, claim 69 or claim 70, wherein said transceiver means comprises page receiving means for receiving a data communication message from said cellular system;

wherein said radiotelephone device is identified by said initial identification number; and

wherein said data communication message comprises said mobile identification number.

72. A wireless telephone which is configured for activation through an activation call originated from a location remote to said wireless telephone, said wireless telephone comprising:

an antenna;

a transmitter which is coupled to said antenna, said transmitter being configured to conduct user information calls;

a receiver which is coupled to said antenna, said receiver being configured to conduct said activation call and said user information calls;

a controller, which is coupled to said transmitter and to said receiver; and

a memory which is coupled to said controller;

wherein said controller is configured to detect a page message received at said receiver during origination of said activation call and referencing a location-independent identifying code stored in said memory.

73. A method for remotely programming a cellular radiotelephone device which includes a programmable memory, said cellular radiotelephone device being programmed with a unique initial identification number, said remotely programming method comprising the steps of:

providing said unique initial identification number to a cellular system;

establishing a data communication session from said cellular system to said cellular radiotelephone device using said unique initial identification number to identify said cellular radiotelephone device;

transmitting data to said cellular radiotelephone device during said session, wherein said data comprises a mobile identification number; and

reprogramming said cellular radiotelephone device so that said cellular radiotelephone device is programmed with said mobile identification number.

74. A method according to claim 73, which includes providing said cellular radiotelephone device with a first memory location for storing a unique telephone serial number, wherein said initial identification number is associated with said telephone number.

75. A method for remotely programming a cellular radiotelephone device which includes a programmable memory which is programmed with a unique initial identification number, said remotely programming method comprising the steps of:

providing said unique initial identification number to a cellular system;

establishing a data communication session from said cellular system to said cellular radiotelephone device using said unique initial identification number to identify said cellular radiotelephone;

transmitting data to said cellular radiotelephone device during said session, wherein said data comprises a mobile identification number; and

reprogramming said programmable memory so that said programmable memory is programmed with said mobile identification number.

76. A method according to claim 75, including the step of providing said radiotelephone device with a non-programmable memory for storing a unique telephone serial number, wherein said initial identification number comprises digits from said telephone number.

77. A method according to any one of claims 73 to 76, which comprises providing said telephone serial number in the form of an electronic serial number of said radiotelephone device.

78. A method according to any one of claims 73 to 76, wherein said providing step further comprises the step of providing said telephone serial number to said cellular system; and wherein said providing step is followed by the step of comparing said telephone serial number and said initial identification number.

79. A method according to any one of claims 73 to 76, wherein said providing step further comprises providing data other than said unique initial identification number to said cellular system.

80. A method according to claim 79, wherein said providing step is followed by the step of controlling the activation of said radiotelephone device.

2182598

1/7

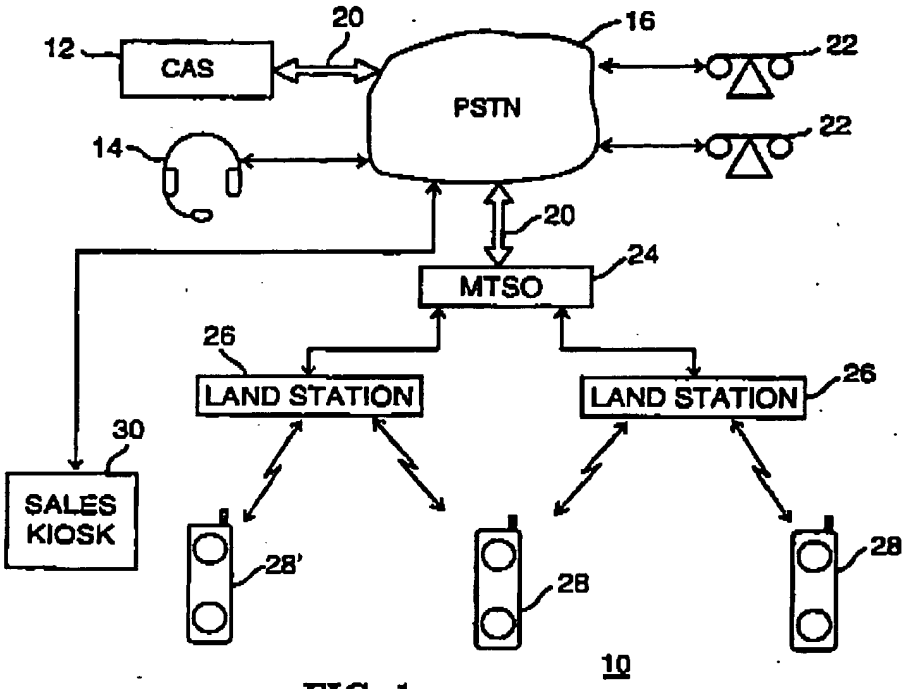


FIG. 1

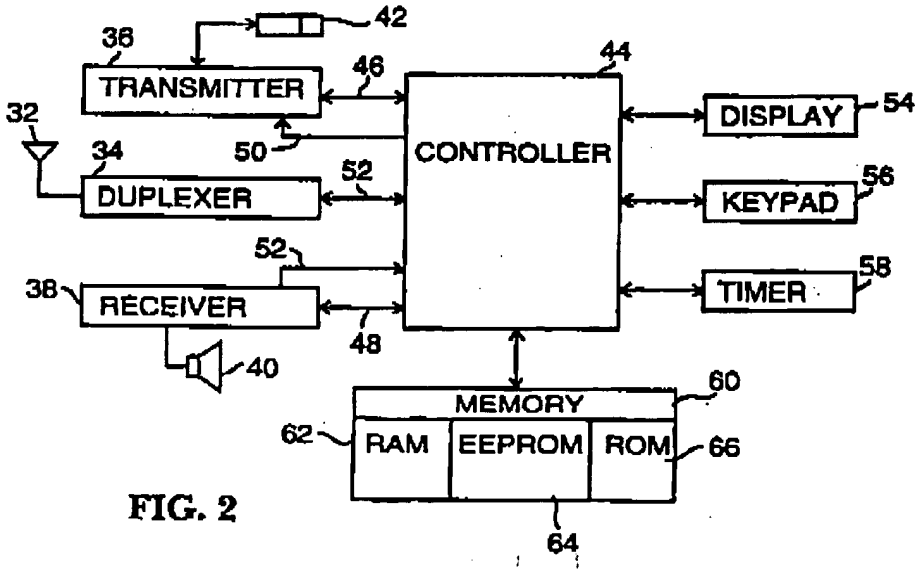
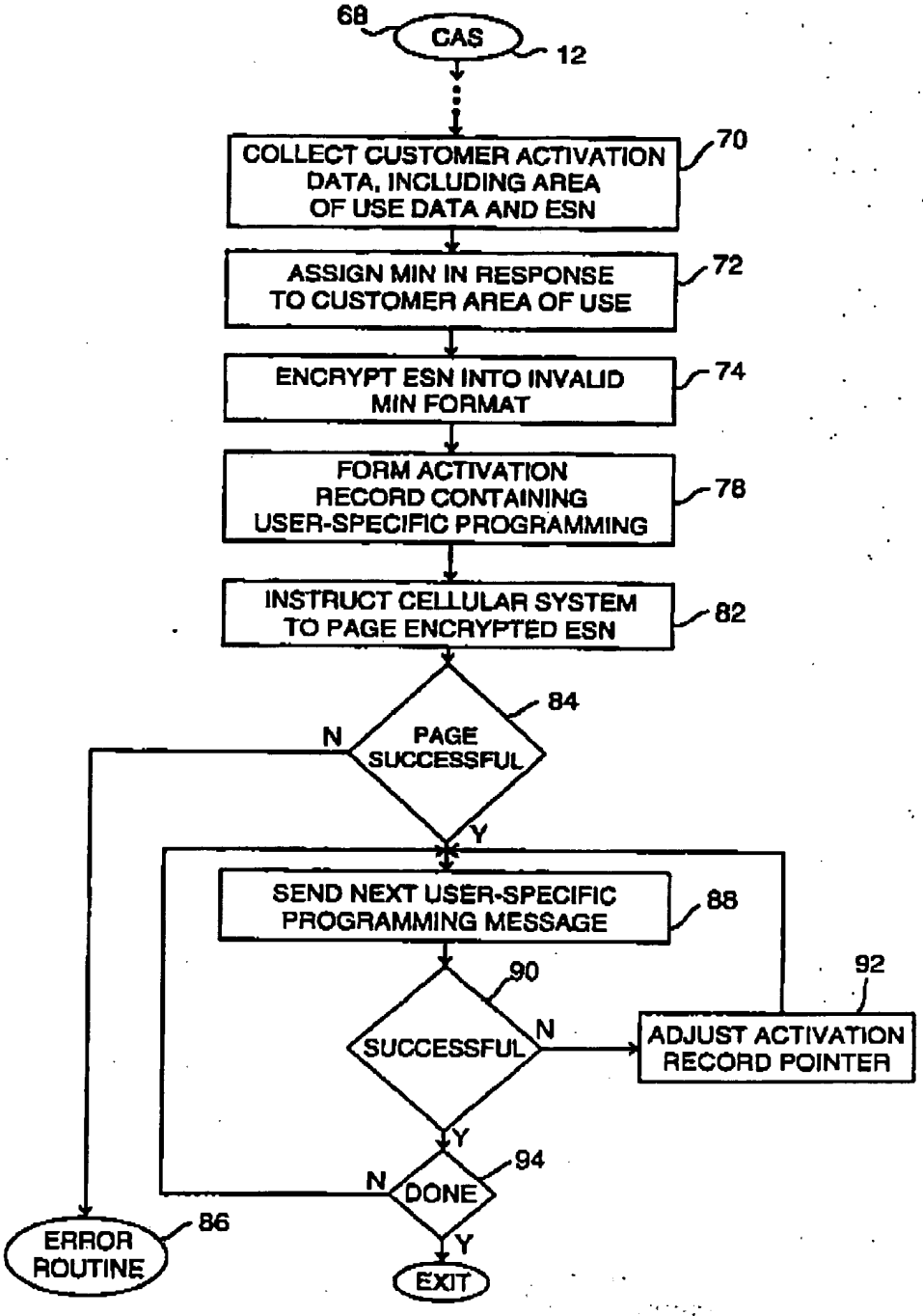


FIG. 2

SUBSTITUTE SHEET (RULE 26)

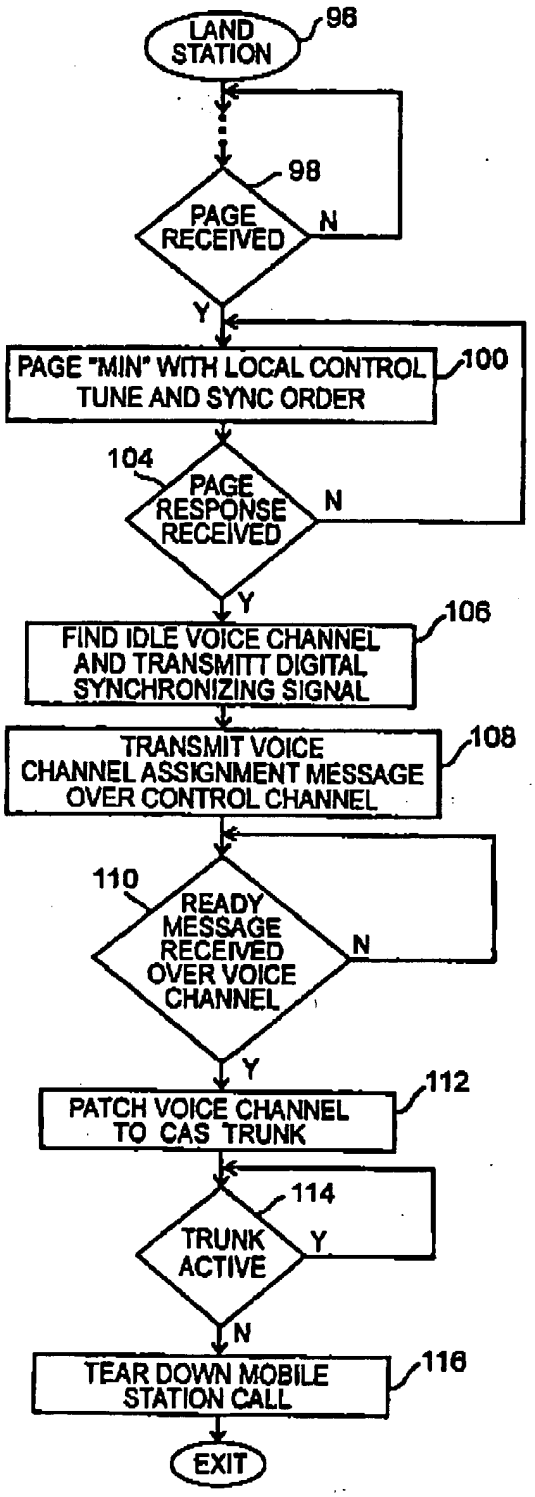
FIG. 3


68
CAS
12
COLLECT CUSTOMER ACTIVATION DATA, INCLUDING AREA OF USE DATA AND ESN
70
ASSIGN MIN IN RESPONSE TO CUSTOMER AREA OF USE
72
ENCRYPT ESN INTO INVALID MIN FORMAT
74
FORM ACTIVATION RECORD CONTAINING USER-SPECIFIC PROGRAMMING
78
INSTRUCT CELLULAR SYSTEM TO PAGE ENCRYPTED ESN
82
84
PAGE SUCCESSFUL
N
Y
SEND NEXT USER-SPECIFIC PROGRAMMING MESSAGE
88
90
SUCCESSFUL
N
92
ADJUST ACTIVATION RECORD POINTER
Y
94
DONE
N
Y
ERROR ROUTINE
86
EXIT

IPEA/US 07 MAR 1996

2162598

FIG. 6



F = 1	NAWC	T	S	E	RSVD = 0	SCM	MIN1 23-0	P
1	3	1	1	1	1	4	24	12

F = 0	NAWC	LOCAL	ORDQ	ORDER	LT	RSVD =	MIN2 33-24	P
1	3	5	3	5	1	000...0	10	12

F = 0	NAWC	SERIAL	P
1	3	32	12

76

FIG. 4

DOTTING	WORD SYNC	REPEAT 1 OF WORD A	REPEAT 1 OF WORD B	REPEAT 2 OF WORD A	...
11	12	44	44	44	

...	REPEAT 4 OF WORD B	REPEAT 5 OF WORD A	REPEAT 5 OF WORD B	DOTTING	...
	44	44	44	44	

DOTTING = 1010101010
WORD SYNC = 11100010010

80

FIG. 5

T_1T_2	DOC	MIN1 23-0	P
1	2	24	12

T_1T_2	SOC= 11 / SOC≠ 11	MIN2 33-24	RSVD =0	LOCAL	ORDQ	ORDER	P
= 10							
2	2	10	1	5	3	5	12

102

FIG. 7

DOTTING	W.S.	REPEAT 1 OF WORD	DOT.	W.S.	REPEAT 2 OF WORD	...
101	11	40	37	11	40	

...	DOT.	W.S.	REPEAT 9 OF WORD	DOT.	W.S.	REPEAT 10 OF WORD	DOT.	W.S.	REPEAT 11 OF WORD
	37	11	40	37	11	40	37	11	40

DOTTING = 1010....101
WORD SYNC = 11100010010 152

FIG. 9

FIG. 8

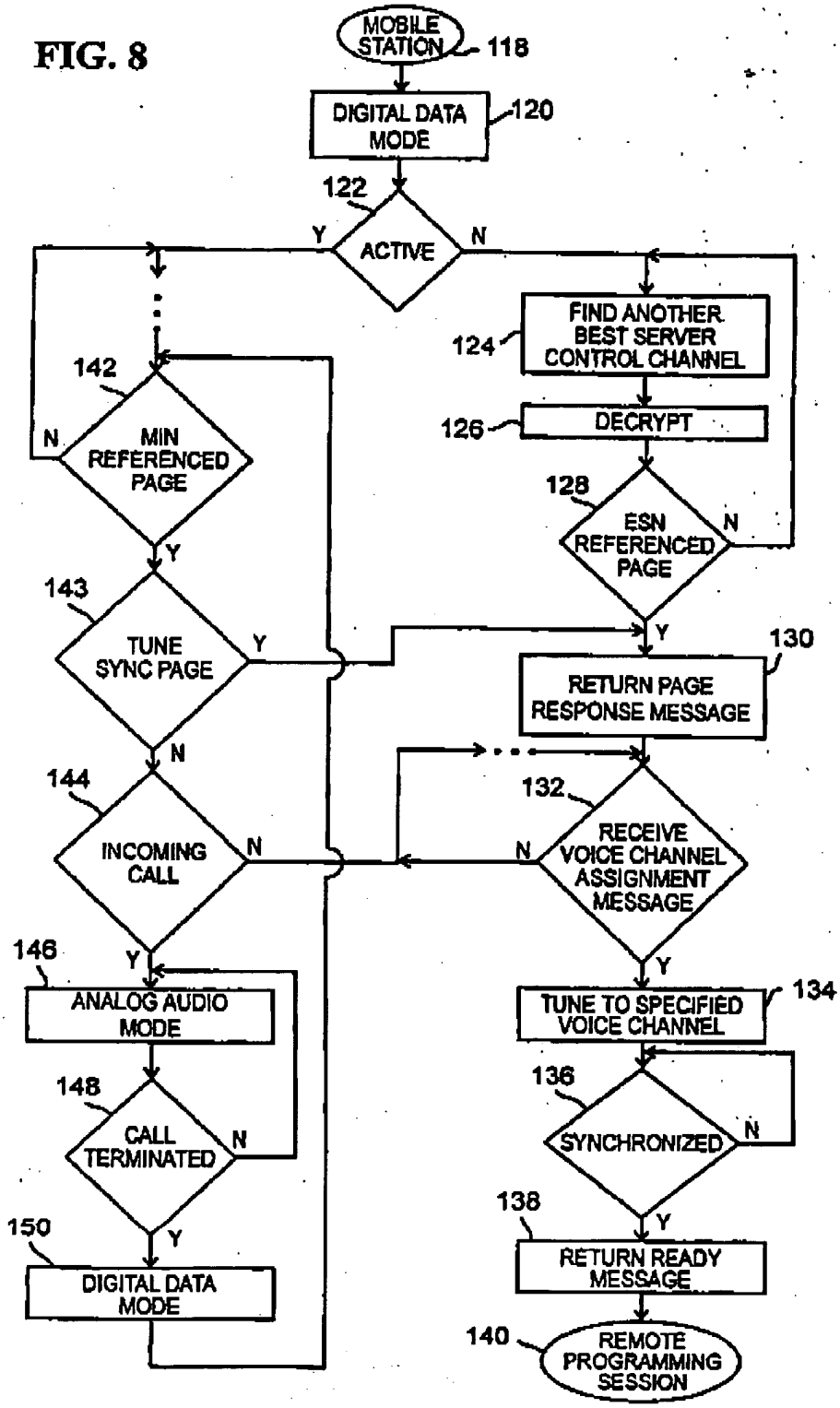


FIG. 10